厚生労働科学研究費補助金

厚生労働科学特別研究事業

安全な保健医療情報流通に向けたネットワークのセキュリティ評価の技術的方策に関する研究

平成１８年度　総括研究報告書

主任研究者　大山　永昭

平成１９（２００７）年　４月

別紙２

目　　次

厚生労働科学研究費補助金（厚生労働科学特別研究事業）

総括研究報告書

安全な保健医療情報流通に向けたネットワークのセキュリティ評価の技術的方策に関する研究

主任研究者　　大山　永昭　　東京工業大学像情報工学研究施設　教授

研究要旨：　今後の医療の高度化やそれに伴う機能分化の促進が想定される状況下で、患者主体の診療が実施されるためには、関連する施設等の間で、電子カルテや医療情報の伝送を安全かつ動的に行っていくための安全なネットワーク基盤が必要である。本研究では、多機能 IC チップを利用し、オープンなネットワーク上で、誰もが安全・手軽に情報サービスを利用可能なネットワーク基盤であるオンデマンド VPN の安全性を実使用環境で検討し、ネットワーク上を流通する医療情報の保護に有効であることを実験的に明らかにした。

分担研究者　　喜多　紘一　東京工業大学像情報工学研究施設 特任教授
近藤　克幸　秋田大学医学部附属病院　教授
山本　隆一　東京大学大学院情報学環　助教授
谷内田　益義　東京工業大学像情報工学研究施設 特任助教授

A．研究目的

近年の情報基盤整備の進展に伴い、保健医療分野における情報化の推進が期待されているが、電子的に保健医療情報の流通を行う場合には、個人情報の保護が極めて重要であり、そのために必要となる適切な措置を講じることが急務とされている。

ここで、個人情報を流通させる上で安全性を確保するためには、医療データ等を使用する者の正当性を認証すること及び、通信回線上や医療機関内での医療データ等の保護を実現することが重要である。これまでに保健医療福祉分野の情報化において必須となる電子的な認証、特に医師･看護婦等の資格認証の必要性の明確化と、電子認証の実施方法や課題の調査・検討が行なわれた。

本研究では、これら研究成果を踏まえ、もう１つの重要な課題である通信回線上で個人情報・医療情報等の安全性を確保する技術について、保健医療分野における情報の安全な流通を確保するネットワーク基盤を構築・運用する際のセキュリティ評価方策について、理論的及び実験的に検討する。これによって、保健医療福祉分野でのネットワーク基盤整備を推進するとともに、それを活用した様々な保健医療福祉サービスの充実が、安全性、利便性、経済性などに優れた技術を用いて提供されることと、保健医療福祉サービスに新たな展開の可能性があること等を明らかにする。

B．研究方法

工学者及び医師らの研究分担者からなる研究班として、医療における情報化推進にあたっている専門家を中心として組織し、委員会を開催して実際に利用されているネットワークサービスの状況や安全性に対する取り組みを調査し、安全な医療情報流通を実現するための課題の抽出と実現方法の検討、及び理論検討と実施調査による上記実現方法の客観的な評価を行い、今後医療分野における共通ネットワーク基盤にするための方策を

検討する。

C．研究結果

(1) 多機能ＩＣチップを利用した安全なネットワーク基盤（オンデマンドVPN）

外出先などからインターネットを使って安全に社内へアクセスすることや、特定の相手に対して安全に情報提供したりするニーズが急速に高まっており、以前は、このようなニーズに対して情報を流通する際のセキュアな通信路の確保手段として、専用線を用いた通信を行っていたが、最近ではコスト面で優れたインターネットなどの公衆回線を利用したVPN(Virtual Private Network)を用いることが多くなってきている。しかし、VPNの構築には、利用者にネットワークの専門知識が必要なうえ、設定などを誤ると情報セキュリティ上多大な影響が発生する恐れがあるなど、誰もが容易に設置できる状況に至っていない。このような背景の下、VPNの状態管理を行うVPN管理機関と2階層PKIに対応したICチップが搭載された通信機器を用いて、利用者の要求に応じて鍵情報などのVPN構築に必要な情報を、ネットワークを介して配送し、即座にVPNが構築可能な環境を構築する多機能ＩＣチップを利用した安全なネットワーク基盤（オンデマンドVPN）の研究開発が進められている。

オンデマンドVPNで利用される多機能ICチップは、住基カードで用いられる広域・多目的ICカードと同等な仕様を持ち、ネットワークに接続された様々な機器の認証に用いることができる。このため、複数の機器間や、異なる組織間で動的に安全なネットワークを構築することができ、ネットワーク上を流通する様々な情報の保護に有効であると考えられる。

保健医療福祉分野においては、医療における情報セキュリティの確保、個人の医療情報の保護などが重要な課題として挙げられているが、オンデマンドVPNで利用されている鍵配送方式は、複数の情報機器間をセキュアなネットワークで繋ぐことを可能とする仕組みであり、インターネットや無線LANなど、ネットワークの種類を問わずセキュリティが確保された状態で情報を流通させることができる。その結果、ネットワーク上を流通する様々な医療情報の保護が可能となる。また、セキュアなネットワークをオンデマンドで構築できる特徴もあることから、電子カルテ等、現在は特定の端末からしか利用できない情報も、旅先で急に病気になってしまったときに現地の端末から必要な認証を経て、自分のカルテ情報等をダウンロードするといったような利用法も考えられる。

現在までに開発され実証実験に供されているオンデマンド VPN は、それぞれ独立した管理機関での運用となっているが、異なる管理機関に属する VPN ルータ同士で接続を行うためには、様々な課題を解決しなければならない。オンデマンド VPN では、ルータ間で IPsec による VPN を構築するために、機器相互の ID や鍵情報などを用いて IPsec-SA を確立する必要があり、現在は、IKE における Pre-Shared Key を利用した鍵交換を採用しているが、このために VPN 通信路毎に異なる鍵が必要となることや、複数の VPN 管理機関間で VPN 通信のローミングサービスを実施する場合の鍵漏洩の危険など、Pre-Shared Key をどのように管理、配送するかが新たな課題となる。このような課題に対して、接続許可証を用いることにより、異なる管理機関同士の接続においても安全な鍵交換を実現する手法が考えられる。まず、証明書ベースの鍵交換を行うためには、現在の Pre-Shared Key による鍵交換ではなくデジタル署名認証方式を導入する。そのためには、秘密鍵およびそれに対応する VPN 管理機関が発行した公開鍵証明書が必要となる。オンデマンド VPN においては、VPN 接続の可否を VPN 管理機関が制御することになるため、IKE 時に必要となる公開鍵証明書の配送を VPN 管理機関が行う。同時に、ルータを管理する VPN 管理機関（機関 A）は、ルータ A への接続許可証を発行し、これを VPN 管理機関 B へ送付する。その後、接続許可証は VPN 管理機関 B から管理下にあるルータ B へ送付される（図 1 参照）。この接続許可証により接続許可の判断や異なる VPN 管理機関へのアクセス権限などを制御する。鍵交換時には、ルータ間で先ほどの接続許可証を交

換し、接続許可証の内容のチェック及び署名検証を行う。仮に、ルータ A 及び B で VPN 管理機関が異なる場合でも、接続許可証の署名検証は自己が属する VPN 管理機関の公開鍵により行うため、IC チップ上で複数の CA の存在を意識する必要はない。この手法では、接続許可証として公開鍵証明書に対応する属性証明書を用いることを想定している。これは、VPN 管理機関発行の属性証明書の送付要求及び証明書送付を Certificate Request ペイロードを利用して送付することが可能なため、従来の ISAKMP パケットの構成と機能をそのまま利用可能であり、既存の鍵交換プロトコルを変更することなく、実現が可能なためである。

今後、これらを医療分野の共通のネットワークインフラとして活用するためには、医療分野におけるネットワークを利用した情報交換のユースケースを明確にし、それぞれの利用形態の特徴抽出・分類・モデル化を行い、それぞれの場合について脅威分析を行い、防止対策とその有効性を確認することが必要である。

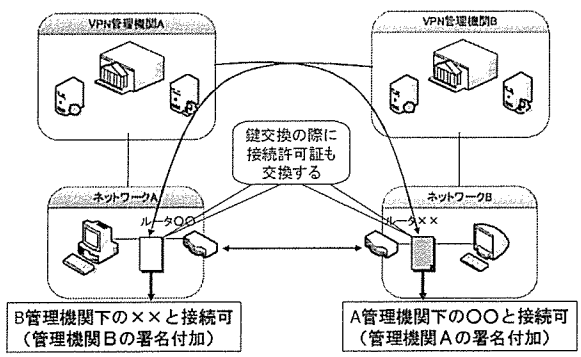

図１．接続許可証を利用した鍵交換

(2) 医療分野におけるユースケースとネットワーク利用形態のモデル化

実地医療において、遠隔地の医療機関間で行いうる医療連携を想定し、まず１医療機関対１医療機関の連携を情報の蓄積と言う観点から４パターンに分類し、各分類につき、ユースケースを抽出した。４パターンとは、（ア）情報の発信側施設にデータが蓄積するタイプ、（イ）情報の受信側施設にデータが蓄積するタイプ、（ウ）共用データセンターを利用するタイプ，（エ）情報の蓄積を伴わないタイプ、の３つである。

（ア）情報の発信側施設にデータが蓄積するタイプ

①．遠隔画像診断

代表的なものに、遠隔病理診断や遠隔放射線画像診断が挙げられる。これらの場合は、発信側施設でデータの蓄積が行われる事になる。

アクタ：発信側施設，受信側施設

概要：発信側施設で取得した病理画像や放射線画像を受信側施設が参照し、読影の上で所見を返送する。

前提条件：遠隔病理診断では、発信側施設はデジタル顕微鏡と画像管理用の DB および画像公開用サーバを、遠隔放射線診断では、発信側施設は PACS を保有する。いずれの場合も受信側施設はビューア（Web クライアントの場合も含む）があり、双方はネットワークで接続される。

イベントフロー：

1) 発信側施設は画像をデジタルデータ化し、患者情報を付加して DB に格納の上、受信側施設に読影依頼する。
2) 受信側施設は発信側施設の DB にアクセスし、画像を参照し、読影の上で所見を入力する（紙媒体での返送もあり得る）。
3) 発信側施設は所見を参照する。

（ネットワークのモデル）

発信側施設が DB を保有し、受信側施設は当該 DB に外部からアクセスし、情報を参照する事となる。

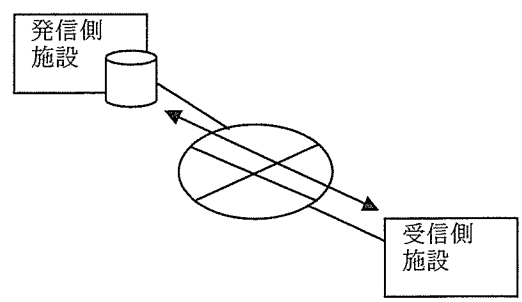

図２　発信側 DB，１対１

なお，受信側施設は必ずしも大規模ではないが、専門医を有する施設となることから、

複数の発信側施設と連携を行う事は十分想定される。従って、地域単位でネットワークを考えた場合は，図３のような構成になる。

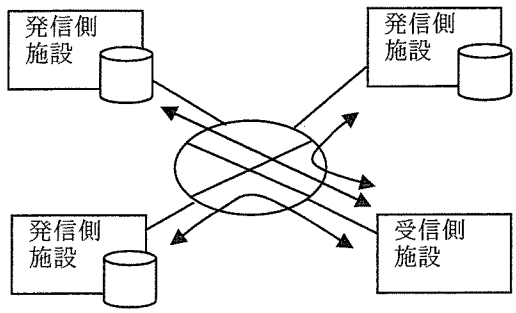

図３　発信側 DB，多対１

このように、複数医療機関が接続する場合は、特に受信側施設においては複数の相手先と双方向性の通信が行われる事となり、それぞれの経路に対する安全性を確保する必要がある。特に Web ベースの診断用クライアントの場合など，複数の発信側施設に対して１台のクライアント機器が共用される事もあり得るので、受信側施設が接続先を任意にコントロールでき、かつそれぞれの通信路の安全性が確保できるような方策が望ましい。

②．患者公開型電子カルテシステム

発信側施設である医療機関が保有する電子カルテシステムの情報を、患者自身にネットワーク経由で公開するタイプのシステムである。

アクタ：発信側施設、患者

概要：発信側施設で入力済みの電子カルテシステムを患者に公開する。

前提条件：発信側施設は電子カルテ（DB）を保有する。患者側はネットワーク経由で自己の情報を参照する手段を有す．双方はネットワークで接続されるが、患者自宅等からのアクセスが多いため、インターネットを利用する。

イベントフロー：

1)　発信側施設は患者情報をデジタルデータとして電子カルテ DB に格納する。

2)　患者はインターネット経由で発信側施設の電子カルテサーバにアクセスする。

3)　患者は自己が受診した時の、自己のデータを参照する（Web 型クライアントが利用される事が多い）。

（ネットワークのモデル）

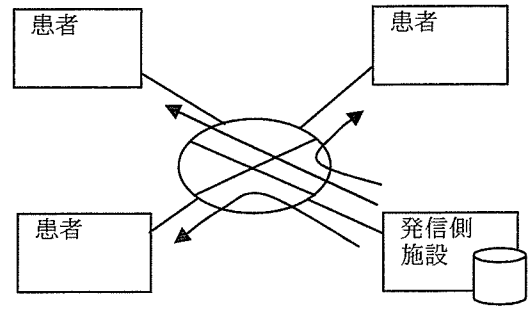

図４　患者公開型電子カルテ

この場合，受信側に相当する患者は多数になる事が多い。また、医療機関のように存在場所の特定が必ずしも固定的ではない。そのため、情報を参照する患者を特定するための手段を十分考慮する必要がある。

（イ）受信側施設にデータが蓄積するタイプ

③　遠隔画像診断

遠隔病理診断については，①項で挙げた画像管理 DB と一体となったデジタル顕微鏡を利用する形態の他に、デジタルカメラを利用して顕微鏡画像をデジタル化し、受信側施設に画像データを送信し、受信側施設で DB に格納する方法もある。

遠隔放射線診断についても同様に、発信側施設でデジタル化された画像データを受診側施設に送信して PACS に格納したり、発信側施設から受信側施設の DICOM サーバに直接 DICOM 通信で書き込む方法などがある。

これらはいずれも、受信側施設にデータが蓄積する形態の遠隔画像診断である。

アクタ：発信側施設，受信側施設

概要：発信側施設で作成した画像データを受信側施設の DB に格納し、受信側施設で読影の上で所見を返送する。

前提条件：発信側施設は画像のデジタル化の手段を有し、受診側施設は画像データを格納する DB を保有する。双方はネットワークで接続される。

イベントフロー：

1) 発信側施設は画像をデジタルデータとし、患者情報を付加して受診側施設に送信する。

2) 受信側施設は受診した画像データをDBに格納する。

3) 受信側施設の専門医が画像を参照し、読影の上で所見を入力する。

4) 発信側施設は所見を参照する（受信側施設がレポート管理サーバを保有し、発信側施設が同サーバを参照する場合、所見参照のユースケースは①項に準ずる）。

（ネットワークのモデル）

受信側施設がDBを保有し、発信側施設は当該DBに外部からアクセスして情報を参照する事となる。

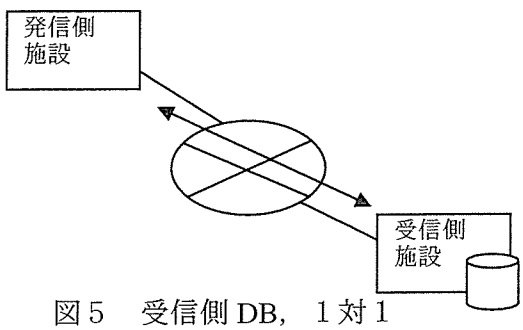

図5　受信側DB，1対1

一般には受信側施設の規模が大きく、外部連携用のサーバを保有し、複数の発信側施設と連携を行う事が多いと思われる。従って、地域単位でネットワークを考えた場合は，下図のような構成になる。

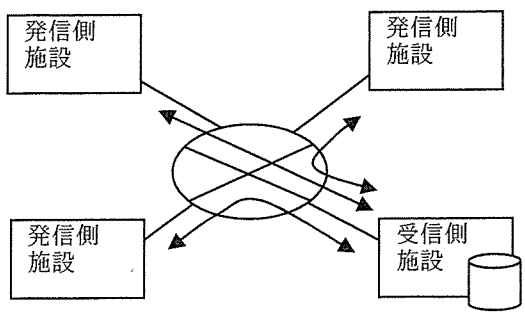

図6　受信側DB，多対1

このような場合は、受信側施設は常時複数施設からの接続を可能としておき、発信側施設が任意に接続をコントロールできる事が必要となる。

④　遠隔画像診断

情報の発信側施設が、例えば患者紹介時の各種情報（病歴、投薬歴、検査データ、画像データなど）を送信し、受信側施設が被紹介施設としてDBにそれらの情報を格納する形態である。この場合は、③項の遠隔画像診断とほぼ同様の形態となる。

アクタ：発信側施設、受信側施設

概要：発信側施設で作成した患者データを受信側施設のDBに格納し、受信側施設では情報を参照し、患者受信時に診察する.

前提条件：発信側施設は各種情報を入力する。受診側施設は患者データを格納するDBを保有する。双方はネットワークで接続される。

イベントフロー：

1) 発信側施設は紹介に必要な情報を入力し、受診側施設に送信する（送信せずに，受信側施設が用意したWeb型情報入力用サーバに発信側施設がアクセスして入力する形態も多い）。

2) 受信側施設は受診した患者データをDBに格納する。

3) 患者受診時または受診前に、受信側施設の医師が情報を参照し、診察する。

（ネットワークのモデル）

この場合、ネットワークのモデルは②項と同様となる。ただし，地域内で複数の医療機関がこのようなモデルに該当する場合は、やや複雑になる。すなわち、発信側施設は唯一の施設に対して紹介するわけではなく、患者の病態や居住地域に応じて複数の受信側施設に対して紹介する可能性がある。また、時として受信側施設が発信側施設になる事もある。従って、その場合のモデルは下図のような構成になる。

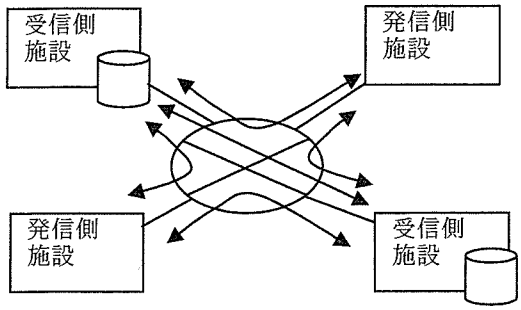

図７　受信側 DB，多対多

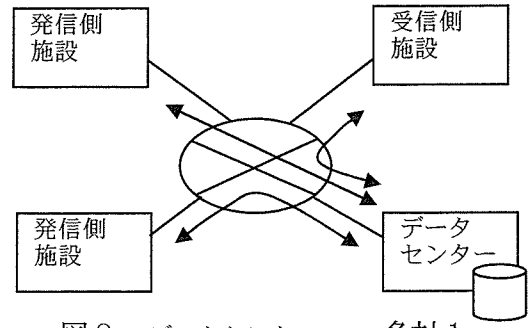

図８　データセンターDB，多対１

（ウ）共有データセンターを利用するタイプ

⑤　共用データセンター型システム

地域の複数医療機関が共用するデータセンターを利用する場合である。情報の発信側施設は、複数医療機関を受診する患者や、他施設への患者紹介時に、各種情報（病歴，投薬歴、検査データ、画像データなど）をデータセンターに送信し、受信側施設が被紹介施設としてデータセンターの情報を参照するタイプである。

アクタ：発信側施設、データセンター、受信側施設

概要：発信側施設で作成した患者データをデータセンターの DB に格納し、受信側施設ではデータセンターにアクセスして情報を参照する．

前提条件：発信側施設は各種情報を入力する．データセンターは患者データを格納する DB を保有する。受信側施設はデータセンターの情報を参照するためのクライアントを保有する。３者はネットワークで接続される。

イベントフロー：

1)　発信側施設は紹介に必要な情報を入力し、受診側施設に送信する．（送信せずに，データセンターが用意した Web 型情報入力用サーバに発信側施設がアクセスして入力する形態も多い）。

2)　データセンターは送信または入力された患者データを DB に格納する。

3)　受信側施設は，必要時にデータセンターにアクセスし，情報を参照する。

（ネットワークのモデル）

このような場合は、データセンターは常時複数施設からの接続を可能としておき、発信側施設が任意に接続をコントロールできる事が望ましい。接続確立時における通信路の安全性確保が必須である。

（エ）情報の蓄積を伴わないタイプ

⑥　遠隔手術支援システム

発信側施設における手術中の画像をリアルタイムに送信し、受信側施設の支援医師がディスプレイ上で参照し，音声や画像でアドバイス等を伝達するシステムである。

アクタ：発信側施設，受信側施設

概要：発信側施設で撮影している動画像または静止画像を送信し、受信側施設はディスプレイで参照，アドバイスを伝達する。

前提条件：発信側施設は動画像または静止画像のデジタル化の手段と送信設備を有し、受診側施設は受信設備を保有する．両者はネットワークで接続される。

イベントフロー：

1)　発信側施設は手術画像を撮影し、デジタルデータとして送信する。

2)　受信側施設は支援医師が受診した画像データを参照する。

3)　受信側施設の支援医師が画像を参照しながらマイクや画像等を利用して、アドバイスを伝える（電話等の通信手段を利用する場合もある）。

（ネットワークのモデル）

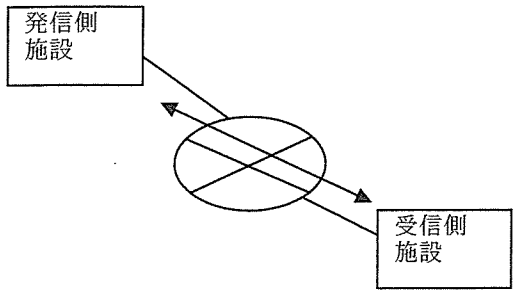

図９　手術支援システム

この場合は、一般に１対１の接続で完結する場合が多い。また、目的とする手術の終了とともに接続が不要となる。

⑦　遠隔カンファレンスシステム

発信側施設はシステムを利用して、動画像に加えてプレゼンテーション用の資料などを送信する。受信側施設は、クライアントアプリケーションで情報を参照する。なお、一般にこの類のシステムは開始時受信側施設からも情報を送信できる場合が多く、必ずしも発信側・受信側と言う分類ができない事が多い。また、発信側施設には接続可能施設情報など、若干の情報を蓄積したサーバを配置している事が多く、厳密には情報を蓄積しないタイプとは言えないが、授受する情報はリアルタイム性を有し、かつＤＢに格納されるものではないため、このタイプに分類した。

（ネットワークのモデル）

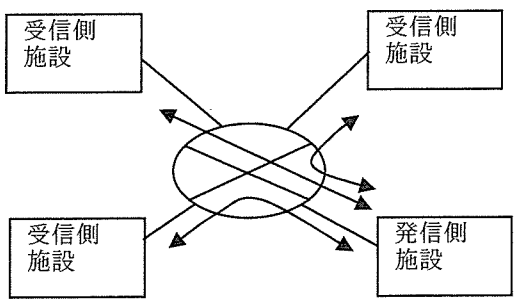

図 10　カンファレンスシステム

（オ）情報の送付タイプ

発信側施設から受診側施設に、一方的に情報が送られるモデルである。具体的には、レセプトのオンライン請求がこのモデルに入ると考えられる。発信側（医療機関）と受診側（保険者）で構成されるＮ対Ｍモデルと、中継期間が介在する中継モデルが想定される。

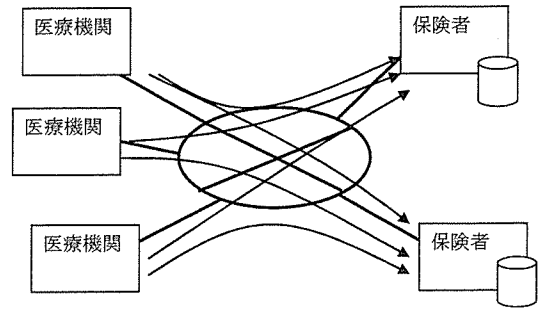

図 11　Ｎ対Ｍモデル

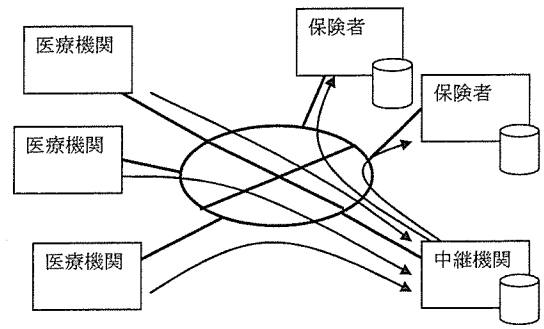

図 12　中継モデル

中継機関は、トラフィックのコントロール、外部との接点を減らすことによる安全性の向上などの理由によって設置され、通常はグループで経営する医療機関などの共通の窓口機能の１つとして提供されるものと考えられる。

(3)　脅威の抽出・防止対策とその有効性

（ア）オンデマンド VPN における脅威と対策

一般には、可用なども含めたネットワークの安全性を考慮する必要があるが、ここでは、プライバシー保護の観点から医療情報をネットワークを介して流通させる際の安全性に焦点を絞って評価を行う。基本的には、基本的には、正しい送り手から正しい受け手に情報資産である患者情報が確実に伝達され、その間にデータの暴露や改変、削除、欠落、すり替えがされないことがもっとも重要な用件である。セキュリティ評価の国際標準である ISO/IEC 15408 の観点からは、

・　データ機密転送保護：送受信される

データの暴露からの保護
- データ完全性転送保護：送受信されるデータの改変、削除、挿入、およびリプレイ攻撃誤りの検出。（受信側のオリジナルデータの回復）
- 高信頼性チャネル：他の通信チャネルとは論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルの提供
- 高信頼性パス：他の通信パスと論理的に区別され、その端点の保証された識別及び改変や暴露からの通信データの保護を提供する通信パスの提供
- 発信の否認不可：発信元を（強制的に）証明
- 受信の否認不可：受信先を（強制的に）証明
- セキュリティ属性によるアクセス制御
- 利用者の識別と認証

等の機能要件を満たすことが必要となる。

オンデマンド VPN を利用した場合の安全性を検討する際以下の 3 つの階層に分けて考えることができる。

1) 医療機関に設置されたルータ間のオンデマンド VPN サービスにより保護される範囲
2) ルータと PC 間の LAN 接続を含む範囲を含む、講義の OD-VPN サービスによる接続範囲
3) 提供される情報流通サービスとして保護すべき範囲

この構成では、以下の脅威を想定することができる。

●インターネット上の脅威

① 第三者による盗聴・改ざん・すり替え

② 不正なエンティティ（機器及び人）による進入

③ 成りすまし

●LAN 上の脅威

④ 許可されていない機器からのアクセス

⑤ 機器の成りすまし

⑥ 許可されていない接続先（機器）への接続

⑦ 不正な利用者の利用

これに対して、以下の対策で対抗することができる。カッコ内は、対応する脅威を示す。前提として、ルータには、それぞれの機関を認証するための鍵と証明書が格納されているものとする。

A) 医療機関に設置されたルータ間の相互認証(②、③)

B) OD-VPN 提供者によるルータ間認証のための鍵配送（②、③、⑥）

C) IKE＋IPSec（ESP トンネルモード）による保護（①）

D) 登録された機器以外でのルータ利用の OD-VPN 接続禁止（②、④、⑤、⑥）

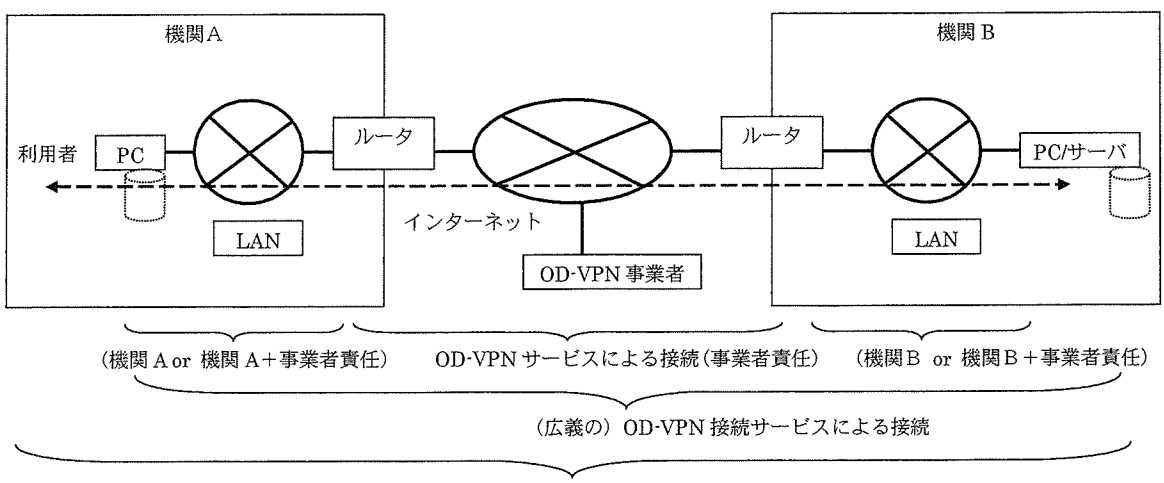

図 11 オンデマンド VPN の構成

E) 正当な機器（ルータ）のオンデマンドVPN提供者への登録（②、④）

OSIのネットワークモデルでのネットワーク層よりも上位のアプリケーション層、つまり接続サービスあるいは特定のアプリケーションで提供する機能での対策は以下を考えることができる。

F) 利用者認証（⑦）

G) セキュリティ属性を付加したアクセス制御(⑦)

H) データレベルでの暗号化（⑦）

2点間を直接接続するモデルでは、以上の脅威と対策で十分であるが、中継機関が存在する場合には、中継機関での脅威に対する対策が必要となる。

●中継機関の脅威

⑧ 許可されていない機器からのアクセス

⑨ 機器の成りすまし

⑩ 許可されていない接続先（機器）への接続

⑪ 不正な利用者の利用

⑫ 悪意を持った操作者による盗聴・改ざん・すり替え

これらの脅威に対しては、

A) 医療機関及び中継機関に設置されたルータ間の相互認証(②、③、⑧、⑨、⑩)

B) オンデマンドVPN提供者によるルータ間認証のための鍵配送(②、③、⑥、⑧、⑨、⑩)

C) IKE＋IPSec（ESPトンネルモード）による保護（①）

D) 登録された機器以外でのルータ利用のオンデマンドVPN接続禁止(②、③、④、⑤、⑥、⑧、⑨、⑩)

E) 正当な機器（ルータ）のOD-VPN提供者への登録(②、④、⑧、⑨、⑩)

F) 利用者認証（⑦）

H) データレベルでの暗号化（⑦、⑫）

となり、通信系路上のデータをアプリケーション（サービス）レベルで暗号化する必要がある。

（イ）オンデマンドVPNと他の接続方式の比較

2点間を安全に結ぶ接続方法としては、オンデマンドVPN以外に専用線、ISDN、IP-VPNなどが存在する。

1) 専用線

2地点（複数点）を論理的に独立したチャネルで結ぶ接続方法である。DSUと呼ばれる接続点の間の接続を事業者が保障する。固定の地点の間の通信に限定される。接続性は保障されるが、悪意を持った関係者による盗聴・改ざん・すり替えなどが想定されるので、アプリケーション層にてデータレベルの暗号化・電子署名などによって機密性・完全性を保障する必要がある。

2) ISDN

任意の2地点を、接続要求に応じてデジタル公衆回線網を利用して接続する方法で、2点間の通信を通信事業者が保障する接続方法となる。接続性は保障されるが、悪意を持った関係者による盗聴・改ざん・すり替えなどが想定されるので、アプリケーション層にてデータレベルの暗号化・電子署名などによって機密性・完全性を保障する必要がある。

3) IP-VPN

通信事業者が提供する通信網、あるいはインターネットを利用したIP通信網の上に、複数の拠点間の通信だけが可能なクローズド名ネットワークを構築する方法である。常時接続の可能な接続方法であり、オープンなネットワーク上に接続する拠点を認証するため鍵情報を共有することとなる。インターネット等オープンなネットワークを利用するので、基本的な脅威・対策は、OD-VPNと同じとなる。

このような医療機関を結ぶ2点間の通信は、医療機関の責任範囲を外れるため、安全な接続が実現できるかどうかが重要となる。OD-VPN,専用線、ISDN、IP-VPNの比較結果が表1である。これらは、成りすまし、盗聴防止、改ざん防止等、機能的には等価な2点間の接続方式と考えられる。但し、安全性を確保するための技術的対策、責任を持つ主体が異なるので、利用者は、コスト・安全性の程度などを考慮し選択する必要がある。

表１　２点間の接続方法の比較

	OD-VPN	専用線	ISDN	IP-VPN
成りすまし防止	OD-VPN 事業者が提供する認証基盤によって２点間の認証を行うことによって対策する。	通信事業者が負い、特定の２点間の通信だけを成立させるので、脅威とならない。	通信事業者が負い、特定の２点間の通信だけを成立させるので、脅威とならない。（番号違いなど、利用者の誤使用による誤った接続を防ぐ対策は必要）	設置期間の管理者、あるいはサービス提供者が設定した認証鍵による認証によって対策する。
盗聴防止	IPSec＋IKE によって保護。暗号の安全性に依存する。 通信上は、事業関係者も第三者も同等に対策される。	第三者の盗聴はない。悪意を持った事業関係者に対する盗聴には、流通する情報の暗号化などの対策で対応可能。	第三者の盗聴はない。悪意を持った関係者に対する盗聴には、流通する情報の暗号化などの対策で対応可能。	IPSec＋IKE によって保護。暗号の安全性に依存する。 通信上は、事業関係者も第三者も同等に対策される。
改ざん防止	IPSec+IKE	通信事業者が保証する	通信事業者が保証する	IPSec+IKE
責任	２点間を結ぶ通信の安全性は、通信事業者（２点間の接続性）と、OD-VPN 事業者（通信の安全性）が負う	通信事業者が負う	通信事業者が負う	通信事業者（２点間の接続性）と設置者（通信の安全性）が負う
その他	サービスの提供を受ける任意２地点間の接続が可能。 オープンなネットワークを利用するので、帯域（スピード）は保証されない。	固定の２地点（多地点）の接続のみ可能 安全性、帯域、接続先は事業者が保証	サービスの提供を受ける任意２地点間の接続が可能。 安全性、帯域（広くはない）、接続先は事業者が保証	固定の多地点の接続可能 オープンなネットワーク上にクローズなネットワークを構築するので、帯域などは保証されない。

(4) 実システムでの評価

オンデマンドVPNを利用した医療情報の実験システムが、加古川市（検査・検診オンラインシステム）と秋田大学病院（遠隔医療診断システム）で稼動している。

（ア）加古川市：検査・検診オンラインシステム

システムは、疾病の早期発見・早期治療、健診の受診率向上を目的とし、各医療機関における個人の健康に関する情報の共有機能やネットワークを介した病診連携機能を提供している。

総合保健センタでは、診療所や小規模病院から検査依頼された検体を検査し、その結果を報告書（紙ベース）にて依頼元の医療機関に報告する。また、オンラインにて、検査結果を加古川地域保健医療情報センタ（以下情報センタと略記）に送付し、管理を委託された情報センタは、検査健診データベースに情報を登録・保存する。

一方、中核病院では、独自で検体の検査を実施し、検査結果を院内の地域医療データベースに登録・保存すると共に、情報センタにオンラインにて送付し、情報センタが検査健診データベースに登録・保存する。

診療所や小規模病院では、総合保健センタより、患者や受診者の検査報告書を紙ベースで受け取ると共に、情報センタの検査健診データベースに登録された医療情報を、オンラインにて検索・参照することができる。

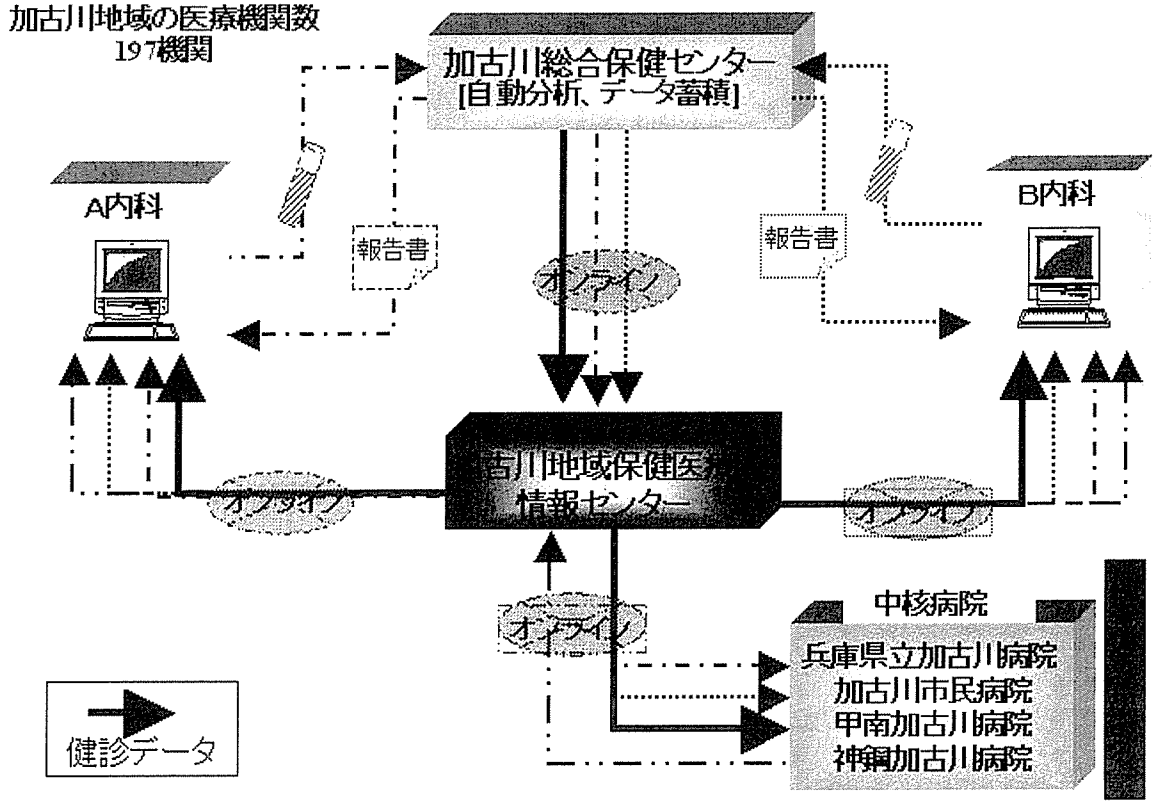

図 12　加古川市検査・健診オンラインシステムの概要

前述のモデルに当てはめると、検査データが総合保険センタと中核病院で検査データが発生し、情報センタの DB に保管･直積するので、受信側 DB 多対 1（図 6）モデルに相当し、診療所・病院からの検査データの参照は、医療機関が情報センタの DB を参照するので、センタ DB 多対 1（図 8）に相当するので、両者を組み合わせたモデルになっている。それぞれの施設を結ぶ 2 点間の通信は、オンデマンド VPN を利用して接続している。

オープンなネットワークに接続されているため、2点間の通信を保護するだけでなく、以下の対策を施している。

- 検査情報などの情報資産を保管するサーバの安全な場所での管理・運用とアクセス制限
- 公開情報のDMZへの配置と、通信の限定
- 外部からDMZ以外へのアクセス禁止
- サービス利用者の認証・限定
- 接続先拠点との合意
- 接続先・接続元のアドレスによるアクセス制限
- 不正な中継禁止
- HTTP、メールアクセスの制限
- ウィルスチェック

これらの対策をオンデマンドVPNと組み合わせることによって、安全なシステム運用を確保している。

（イ）秋田大学：遠隔医療診断システム

秋田大学付属病院を中心とした遠隔診断の取り組みでは、医師・専門医不足対策と、地域医療の向上を目的として、遠隔画像読影ネットワークが稼動している。このシステムは、遠隔画像読影ネットワークと、医療画像読影依頼・レポートシステムで構成し、地域の小規模病院や診療所で撮影されたCTやMRIの画像の読影を、専門医のいる大規模・中核病院や大学病院に依頼し、専門医が読影を行って、その結果をレポートとして返送することで、専門医不足の解消や地域医療の向上を図ろうとするものである。

秋田大学病院側で、小規模病院からの画像

を登録する連携データベースと、読影結果のレポートを蓄積する読影依頼・レポートシステムが稼動し、外部医療機関からアクセスできるようになっている。2つのシステムから構成されており、前述のモデルに当てはめると、読影画像データの蓄積が受信側DB多対１（図６）モデルに相当し、読影レポートの参照がンタDB多対１（図８）に相当する。秋田大学病院と外部医療施設を結ぶ2点間の通信は、オンデマンドVPNを利用して接続している。

オープンなネットワークに接続されているため、2点間の通信を保護するだけでなく、以下の対策を施している。

- 検査情報などの情報資産を保管するサーバの安全な場所での管理・運用とアクセス制限
- 公開情報のDMZへの配置と、通信の限定
- 外部からDMZ以外へのアクセス禁止
- サービス利用者の認証・限定
- 接続先拠点との合意
- 接続先・接続元のアドレスによるアクセス制限
- 不正な中継禁止
- HTTP、メールアクセスの制限
- ウィルスチェック

これらの対策をオンデマンドVPNと組み合わせることによって、安全なシステム運用を確保している。

D．考察

近年、様々な診療情報を医療施設や患者等の間でネットワークを介して電子的に交換・共有する試みが行われているが、個人情報保護のために専用回線等を通じ、あらかじめ固定された施設間における限定的な運用がなされていることが多い。しかしながら、今後、更なる医療の高度化やそれに伴う機能分化の促進が想定され、このような状況下で患者主体の診療が実施されるためには、関連する施設等の間で、医療情報の伝送を安全かつダイナミックに行っていくためのネットワーク基盤が必要である。

また、医療情報の伝送を行う際には、電子署名法やe-文書法等などの新たな制度への対

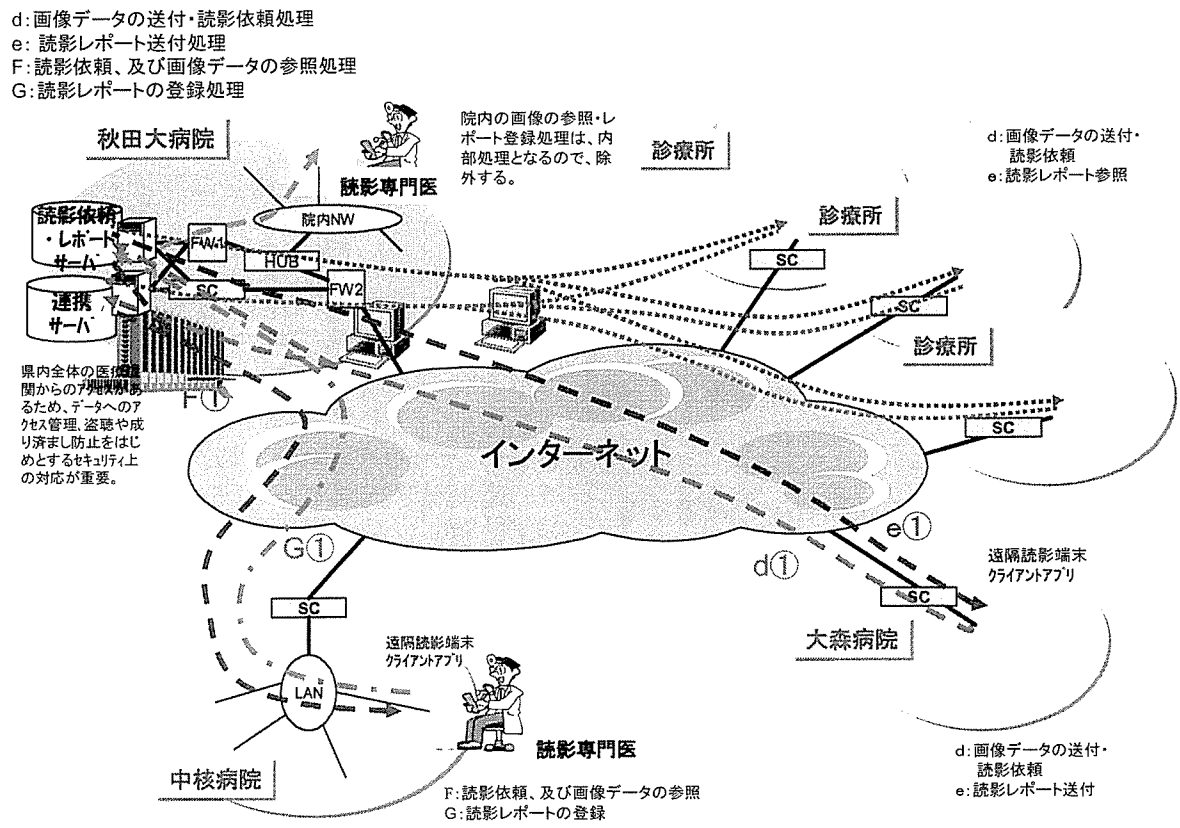

図 13　秋田大学病院の連携システム概要

応や情報セキュリティの確保及び個人情報保護の実現を必須要件とし、医療施設におけるセキュリティ対策、ネットワーク上の安全な情報伝達、情報の真正性保証等を実現する保健・医療・福祉分野における共通的な技術的基盤を構築すべきである。ここで、オンデマンドVPNは、利用者や利用環境をネットワーク経由で迅速に確認し、複数の情報機器で動的にセキュアなネットワークを構築することができることから、医療分野における共通的なネットワーク基盤の候補として有効である。

オンデマンドVPNの安全性は、IP-VPNと等価であり、機能的には、専用線やISDNなどの方法と同じ安全性を提供することがわかった。ネットワークの拡張性、接続先の柔軟性、コストなどによって、利用者となる医療機関がそれぞれの選択によって決定できる環境を整備することが重要である。また、複数のネットワーク基盤が利用された場合や、将来予想されるNGNなどのネットワーク基盤を前提に、複数の基盤の共存や新しい基盤への移行を念頭に置いた医療ネットワーク基盤を構築して行くことも重要である。

また、中継点が入る場合など、2点間の通信で医療機関の管理が及ばない構成をとる場合、医療機関の責任で流通する情報の機密性・完全性を保障するためには、アプリケーションレベルでの暗号化・電子署名等の付与が必要となる。

さらに、今後はネットワーク基盤の整備とともに、それを活用した様々な保健医療福祉サービスの充実が求められており、ネットワーク基盤を利用した安全性、利便性、経済性などに優れた医療サービスの具体的検討が必要である。

E．結論

本研究では、保健医療福祉分野の情報流通に向けたネットワークセキュリティの評価技術を検討し、医療でのユースケースでの検討、実使用システムでの評価を通じて、オープンなネットワークを利用する流通基盤であっても、OD-VPN等のように一定の安全性を確保する手法を用いれば、医療情報流通に問題がないことを確認した。また、情報を流通する経路に通信事業者や中継機関など医療機関外が責任を持つ範囲の存在する場合には、医療機関の責任で情報を保護するために、通信層よりも上位のアプリケーション層にて暗号化・電子署名等の対策をすることで情報の機密性・完全性を実現する必要があることも示した。

本研究で得られた成果は、安全なネットワーク基盤を利用した保健医療福祉サービスの研究開発に活用される予定となっている。具体的には、保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアムや現在オンデマンドVPN技術の研究開発を行っている研究グループとの間で成果を共有することで、これら研究グループが進めている医療機関相互における情報連携の実証実験や医療サービスの検討等への反映や、オンデマンドVPNを構成する技術仕様へフィードバックすることを予定している。

さらに、ネットワーク基盤の整備だけでなく、それを活用した様々なサービスの拡充が求められており、今後、本研究で得られた成果を活用して、新たな保健医療福祉サービスに関する研究開発が行われることを期待する。

F．健康危険情報

該当なし

G．研究発表

1．論文発表

- 大山永昭：医療機関における個人情報保護とセキュリティシステム；日本病院会雑誌，53(10)，118-136(2006)

2．学会発表

- 小尾高史，鈴木裕之，谷内田益義，山口雅浩，大山永昭：多機能 IC チップを利用した任意多地点間 VPN のための鍵交換手法；ワイヤレス・テクノロジーパーク 2006 講演予稿集，20-21(2006)
- 押田知己，谷内田益義，鈴木裕之，小尾高史，山口雅浩，大山永昭：多機能 IC チップを利用したネットワークサービスにおける暗号技術の更新とサービスの継続利用の実現；電子情報通信学会 2007 年総合

大会講演予稿集，225(2007)
- 浦野雄平,小尾高史，大山永昭，谷内田益義，鈴木裕之：多機能 IC チップを利用した任意多地点間 VPN における通信主体情報の秘匿；電子情報通信学会 2007 年総合大会講演予稿集，230(2007)

安全な保健医療情報流通に向けたネットワークのセキュリティ評価の技術的方策に関する研究・分担研究報告書

脅威の抽出・防止対策の有効性検討

分担研究者
喜多　紘一・谷内田　益義
東京工業大学・像情報工学研究施設

１．研究の背景、目的

任意 2 地点間を結ぶためのセキュアネットワーク基盤として、オンデマンド VPN（OD-VPN）が実用化され、２地点間を安全に結ぶための基本的技術課題が解決している。本研究は、医療分野におけるユースケースを念頭に、以下を目的としている。

- ネットワークサービスの安全性を、ユースケースに基づいたモデル化とシステム用件の抽出・明確化
- 実用環境を利用した実証実験を通した検証

本報告では、想定するモデル、脅威の抽出、防止対策の有効性の検討の現状を報告する。

２．医療分野における利用形態

以下の３つを代表例として想定する。

１）地域連携

複数の医療機関で互いに接続して患者情報の共有を図るための利用で、患者情報の蓄積を伴う。地域の中核医療施設が DB を構築する場合、各医療施設が DB を構築する場合などが想定される。情報は、双方が送受信する可能性がある。

① 分散 DB モデル：グループ内（関連医療施設）任意２地点間の接続

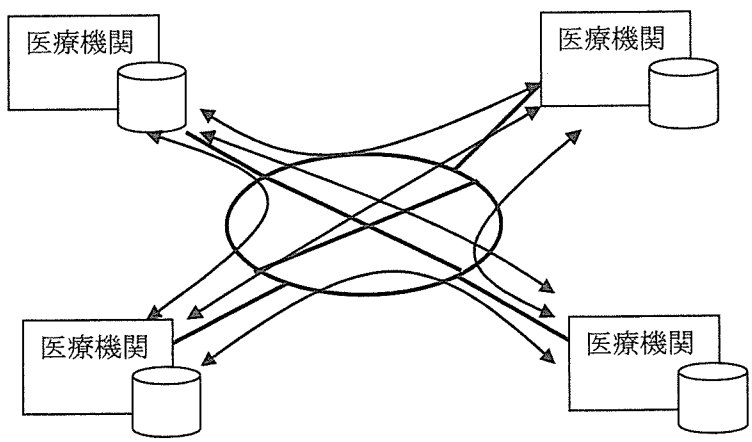

図１　分散ＤＢモデル

② 集中 DB モデル：１対多地点間の接続

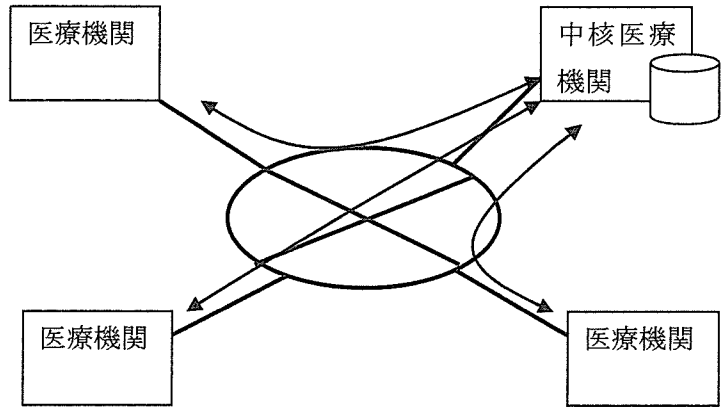

図２　集中ＤＢモデル

２）遠隔医療

２医療を結ぶための利用で、基本的には情報の蓄積は伴わない

③ 分散モデル：グループ内（中核医療施設と関連医療施設）の中核病院と任意医療施設間の２地点間の接続

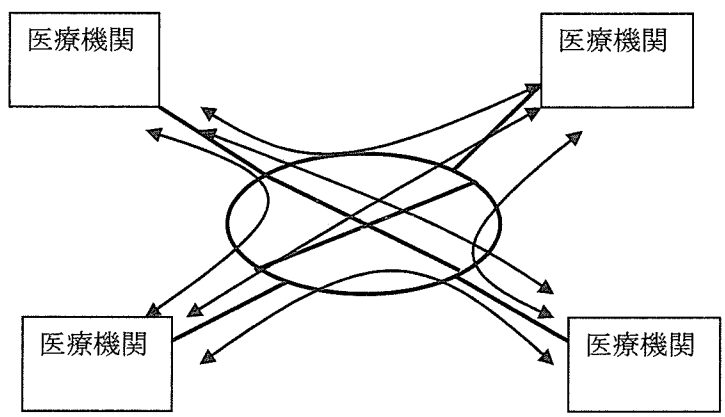

図３　分散モデル

３）レセプトのオンライン請求

中央 DB に情報を送信する利用

④ Ｎ対Ｍモデル：個々の医療関連機関から複数の保険者にレセプト情報を送付する

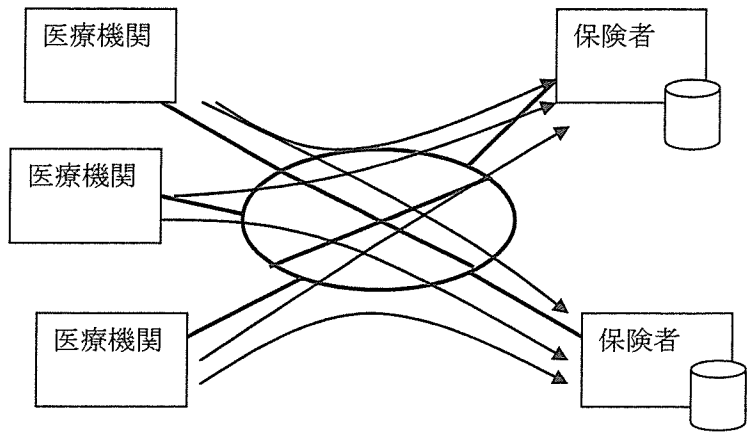

図４　Ｎ対Ｍモデル

⑤ 中継モデル：グループ内の医療関連施設から、中継施設を経由して、複数の保険者にレセプト情報を送付

中継機関を設ける理由は、トラフィックのコントロール、外部との接点を減らすことによる安全性の向上などの理由が考えられる。

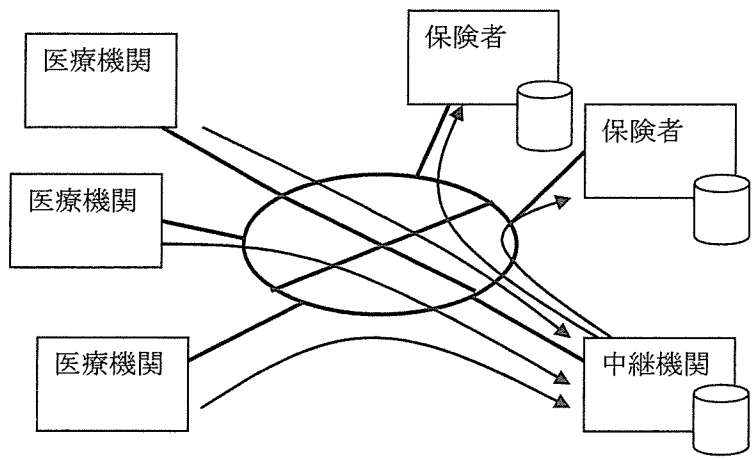

図５　中継モデル

３．ネットワークに要求されるセキュリティ要件

一般には可用性などを確保するために、DOS 攻撃への対抗、障害への耐性などを考慮しなくてはならないが、本研究では、これらの一般的なセキュリティ要件を別として、医療情報をネットワークを介して流通させるために必要となる要件をまとめる。考慮すべきなのは、医療機関が取り扱う情報はプライバシー情報であるため、プライバシー保護の観点から重要な用件をまとめる必要がある。基本的には、正しい送り手から正しい受け手に情報資産である患者情報が確実に伝達され、その間にデータの暴露や改変、削除、欠落、すり替えがされないことがもっ

とも重要な用件である。セキュリティ評価の国際標準である ISO/IEC 15408 の観点からは、

- データ機密転送保護：送受信されるデータの暴露からの保護
- データ完全性転送保護：送受信されるデータの改変、削除、挿入、およびリプレイ攻撃誤りの検出。（受信側のオリジナルデータの回復）
- 高信頼性チャネル：他の通信チャネルとは論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルの提供
- 高信頼性パス：他の通信パスと論理的に区別され、その端点の保証された識別及び改変や暴露からの通信データの保護を提供する通信パスの提供
- 発信の否認不可：発信元を（強制的に）証明
- 受信の否認不可：受信先を（強制的に）証明
- セキュリティ属性によるアクセス制御
- 利用者の識別と認証

等の機能要件を満たすことが必要となる。

4．各利用形態における脅威と技術対策

4．1　基本的な OD-VPN 構成

OD-VPN を利用する際、基本的には以下の構成で安全性を検討する必要がある。

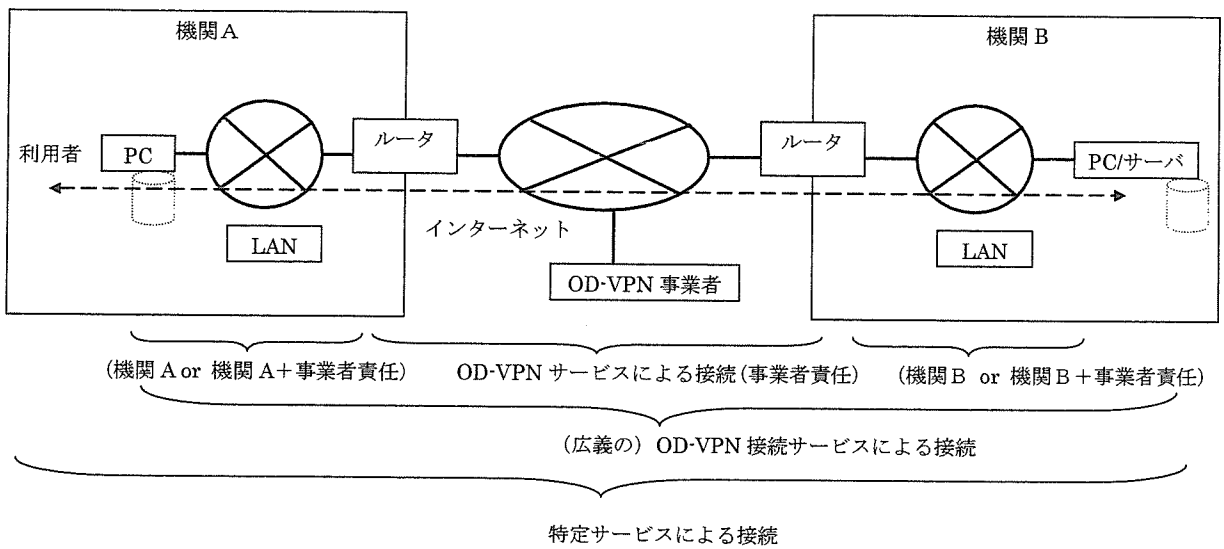

図６　OD-VPN を利用した基本構成

階層として考えると、以下の３つの階層に分けて考えることができる。

1）ルータ間の OD-VPN サービスにより保護すべき範囲
2）ルータと PC 間の LAN 接続を含む範囲を含む、講義の OD-VPN サービスによる接続範囲
3）提供される情報流通サービスとして保護すべき範囲

このような基本構成をとる場合には、以下のような脅威を想定することができる。

●インターネット上の脅威

① 第三者による盗聴・改ざん・すり替え